Identity Based Multicloud Data Possession

[1]Y MeenaPriyadarshini, [2]Dr.P S K Patra,[3]S Prakash
[1]Student, [2]Professor & Head, [3]Assistant Professor
Agni College of Technology, Chennai, India

Abstract **- Far-off data correctness checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, I propose a novel remote data integrity checking model: APDP (Agent-based provable data possession) in multi-cloud storage. The formal system model and security model are given. The cloud server act as a container which contains data or information. In this proposed system we can send the file with authentication by encrypting and chunking to partitions. One can retrieve the data from multiple cloud as chunks and then merge it together by mining the key file then decrypt method is used to view the file. APDP protocol can realize private verification, delegated verification and public verification proposed method on the achievable security merits by making use of multiple distinct clouds simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects. Also I proposed the splitting and merging concepts during storage in cloud environment.**

IndexTerms **- Multi cloud, Agent, Data Possession, Chunks.**

I. INTRODUCTION

Over the last years, cloud computing has become an important theme in the computer field. Essentially, it takes the information processing as a service, such as storage, computing. It relieves of the burden for storage management, universal data access with independent geographical locations. At the same time, it avoids of capital expenditure on hardware, software, and personnel maintenances, etc. Thus, cloud computing at- tracts more intention from the enterprise. The foundations of cloud computing lie in the outsourcing of computing tasks to the third party. It entails the security risks in terms of confidentiality, integrity and availability of data and service. The issue to convince the cloud clients that their data are kept intact is especially vital since the clients do not store these data locally.

Remote data integrity checking is a primitive to address this issue. For the general case, when the client stores his data on multi-cloud servers, the distributed storage and integrity checking are indispensable. On the other hand, the integrity checking protocol must be efficient in order to make it suitable for capacity-limited end devices. Thus, based on distributed computation, we will study distributed remote data integrity checking model and present the corresponding concrete protocol in multi-cloud storage. In this project we proposed a shared access authority based on the client's authorization the proposed protocol can realize private verification, delegated verification and public verification in Multi-Cloud Storage.

The basic underlying idea is to use multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering. By integrating distinct clouds, the trust assumption can be lowered to an assumption of non-collaborating cloud service providers. These cloud security issues and challenges triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Alongside with these security issues, the cloud paradigm comes with a new set of unique features that open the path toward novel security approaches, techniques, and architectures.

II. RELATED WORK

Authors : Huifeng Wang, Xi'an, Zhanhuai Li , Xiao Zhang ; Jian Sun more authors
Title : A Delayed-Update Provable Data Possession in the Cloud
Year : 2014

Description: This paper introduces a model for a delayed-update provable data possession (DU-PDP) that allows clients adopting delayed-update policy to verify the integrity of their own data stored in the cloud. Compared with other similar PDP models, it can efficiently support dynamic data. The one of the security issue Integrity alone checked here.

Authors : Huifeng Wang, Xi'an, Zhanhuai Li , Xiao Zhang; Jian Sun more authors
Title : Proxy Provable Data Possession in Public Clouds
Year : 2012

Description: In this paper, they proposed a new protocol proxy provable data possession (PPDP). In public clouds, PPDP is a matter of crucial importance when the client cannot perform the remote data possession checking. We study the PPDP system model, the security model, and the design method. Based on the bilinear pairing technique, we design an efficient PPDP protocol. The chances of data getting spoofed while travelling through the medium.

Authors : Chaoling Li , Yue Chen , Pengxu Tan , Gang Yang
Title : An Efficient Provable Data Possession Scheme with Data Dynamics
Year : 2012

Description: To achieve full data dynamics, a SN-BN table which maps the logical indices of blocks to their physical ones is introduced. The SN (Serial Number) is used to determine which blocks are included in tags, while the corresponding BN (Block Number) is used to retrieve the actual data blocks. Therefore, it can support full data dynamics including block modification, deletion, and insertion and appending. But there is no special care on security issues.

III. SYSTEM ARCHITECTURE

In cloud computing, remote data integrity checking is an important security problem. The clients' massive data is outside his control. The malicious cloud server may corrupt the clients' data in order to gain more benefits. The formal system model and security model are existing models. In the PDP model, the verifier can check remote data integrity with a high probability. Based on the RSA, they designed two provably secure PDP schemes. PDP allows a verifier to verify the remote data integrity without retrieving or downloading the whole data. It is a probabilistic proof of possession by sampling random set of blocks from the server, which drastically reduces I/O costs. The verifier only maintains small metadata to perform the integrity checking. PDP is an interesting remote data integrity checking model.

In POR, the verifier can check the remote data integrity and retrieve the remote data at any time. On some cases, the client may delegate the remote data integrity checking task to the third party. It results in the third party auditing in cloud computing. Risk management and (legal) compliance issues must be well defined in the contract between multi- Cloud Computing provider and customer and should enable transparency with regard to the processing and storage of data.

The service provided shall be compliant with the regulation and legislation that the customer needs to follow, and also customers should be enabled to be compliant with the respective regulation and legislation. An open and clear specification of the measurements taken to ensure the security the phase Extract, PKG creates the private key for the client. The client creates the block-tag pair and uploads it to combine. The combiner distributes the block-tag pairs to the different cloud servers according to the storage metadata. The verifier sends the challenge to combiner and the combiner distributes the challenge query to the corresponding cloud servers according to the storage metadata.

The cloud servers respond the challenge and the combiner aggregates these responses from the cloud servers. The combiner sends the aggregated response to the verifier. The telecommunications network that supports the cloud computing services should be secured and protected against malware and DOS attacks. Secure storage using splitting and merging concepts in cloud storage environment.

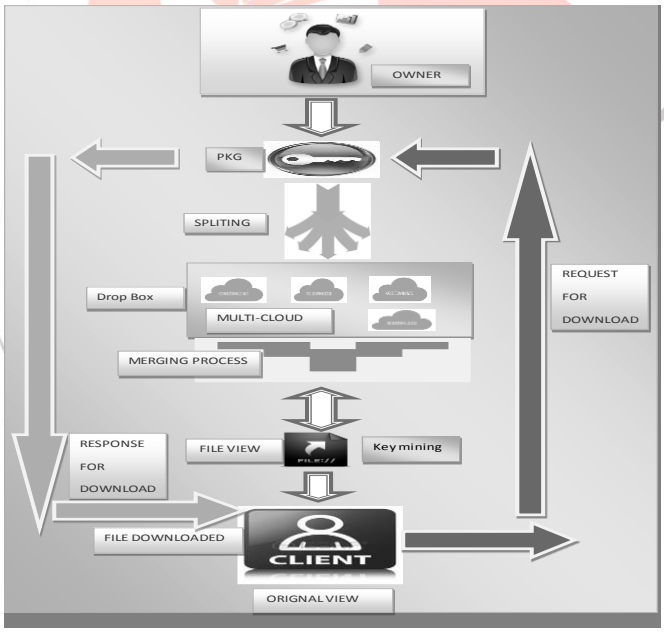

Figure 1.System Architecture

In cloud computing, remote data integrity checking is an important security problem. The clients' massive data is outside his control. The malicious cloud server may corrupt the clients' data in order to gain more benefits. The formal system model and security model are existing models. In the PDP model, the verifier can check remote data integrity with a high probability. Based on the RSA, they designed two provably secure PDP schemes. PDP allows a verifier to verify the remote data integrity without retrieving or downloading the whole data. It is a probabilistic proof of possession by sampling random set of blocks from the server, which drastically reduces I/O costs. The verifier only maintains small metadata to perform the integrity checking. PDP is an interesting remote data integrity checking model.
In POR, the verifier can check the remote data integrity and retrieve the remote data at any time. On some cases, the client may delegate the remote data integrity checking task to the third party. It results in the third party auditing in cloud computing. Risk

management and (legal) compliance issues must be well defined in the contract between multi- Cloud Computing provider and customer and should enable transparency with regard to the processing and storage of data.

The service provided shall be compliant with the regulation and legislation that the customer needs to follow, and also customers should be enabled to be compliant with the respective regulation and legislation. An open and clear specification of the measurements taken to ensure the security the phase Extract, PKG creates the private key for the client. The client creates the block-tag pair and uploads it to combine. The combiner distributes the block-tag pairs to the different cloud servers according to the storage metadata. The verifier sends the challenge to combiner and the combiner distributes the challenge query to the corresponding cloud servers according to the storage metadata.

The cloud servers respond the challenge and the combiner aggregates these responses from the cloud servers. The combiner sends the aggregated response to the verifier. The telecommunications network that supports the cloud computing services should be secured and protected against malware and DOS attacks. Secure storage using splitting and merging concepts in cloud storage environment.

IV. PROPOSED METHODOLOGY

Multi-cloud architecture specifies that the application data is partitioned and distributed to distinct clouds as shown in figure 5.1. The most common forms of data storage are files and databases. Files typically contain unstructured data (e.g., pictures, text documents) and do not allow for easily splitting or exchanging parts of the data. This kind of data can only be partitioned using cryptographic methods.

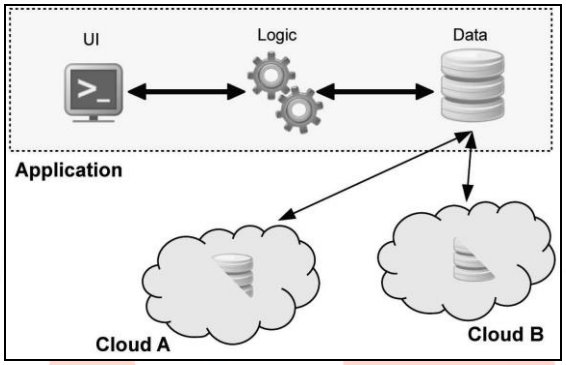

Figure 2 Multi-cloud Data Partition

Databases contain data in structured form organized in columns and rows. Here, data partitioning can be performed by distributing different parts of the database (tables, rows, columns) to different cloud providers. Finally, files can also contain structured data (e.g., XML data). Here, the data can be split using similar approaches like for databases. XML data, for example, can be partitioned on XML element level. However, such operations are very costly. Thus, this data are commonly rather treated using cryptographic data splitting

This protocol comprises four procedures: Setup, Extract, TagGen, and Proof. Its architecture can be depicted in Figure 2. The figure can be described as follows: In the phase Extract, PKG creates the private key for the client. The client creates the block-tag pair and uploads it to combiner. The combiner distributes the block-tag pairs to the different cloud servers according to the storage metadata. The verifier sends the challenge to combiner and the combiner distributes the challenge query to the corresponding cloud servers according to the storage metadata. The cloud servers respond the challenge and the combiner aggregates these responses from the cloud servers. The combiner sends the aggregated response to the verifier. Finally, the verifier checks whether the aggregated response is valid.

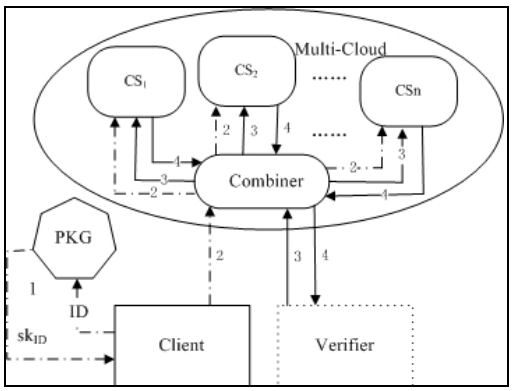

Figure3. APDP Protocol Architecture

The concrete APDP construction mainly comes from the signature, provable data possession and distributed computing. The signature relates the client's identity with his private key. Distributed computing is used to store the client's data on multi-cloud

servers. At the same time, distributed computing is also used to combine the multi-cloud servers' responses to respond the verifier's challenge.

V. RESULTS AND DISCUSSION

Existing technique such as Eliminating Threats during PDP [5] shows that static analysis is processed by using SQL Graph representation using FSM. In AMNESIA [4] static model build SQL-query models**:** For each hotspot, build a model that represents all the possible SQL queries that may be generated at that hotspot. A *SQL-query model* is a non-deterministic. The table I compares the techniques on three factors they execution time, speed and support in various platforms.

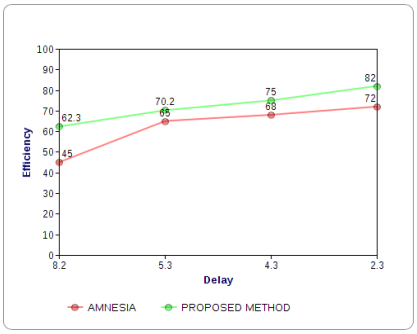

Figure 4. Performance Analysis

Figure 2 illustrates the efficiency for proposed method. It shows the raise in delay does not affect the efficiency of proposed system.

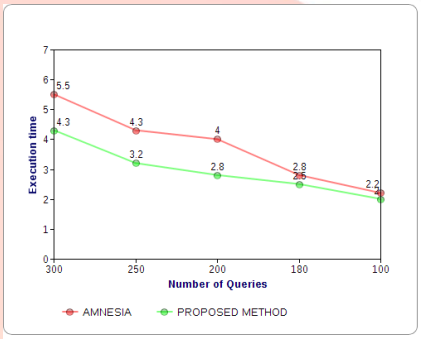

Figure 5. Speed Analysis

Here we compared the proposed technique with AMNESIA based on number of queries they can process per second. The current technique can able to concentrate on 300 queries per second with less execution time.

The existing techniques [17] [18] are fully Query based validation but the current technique is data based validation using artificial intelligence concepts and Runtime validation to secure the web application. The execution time shows that the current technique results a better performance than existing mechanism as well as the computational cost is also minimum compared to this existing mechanism.

The proposed Intelligent System developed for SQL Server, MS Access and Big data. The detection overhead and prevention overhead is calculated The Figure 6 (a) and (b) provides comparison chart for detection and prevention overhead for the proposed technique with query based technique [5] [8]. The following equation is used for calculating detection and prevention overhead.

Detection Overhead = Tdetection/Tround-trip

Where Tdetection is time needed for detecting malicious characters in the user input and Tround-trip is the response time for completing a MDX query. Detection overhead is measured in 5 web sites for the three techniques and the average overhead is displayed Table 2.

Technique	**Detection Overhead**
Intelligent System	5.1

SQLiX	6.2
AMNESIA	8.5

Table II Detection Overhead Comparison

The Table II shows that detection overhead is very less for the proposed system.

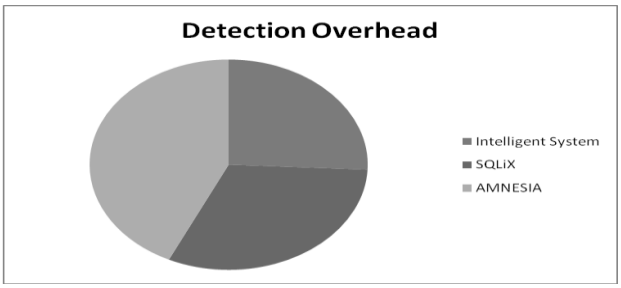

Figure 6. Detection Overhead

The calculated detection overhead value is compared with 2 other techniques and in the proposed system the overhead is very less.

VI. CONCLUSION AND FUTURE WORK

In multi-cloud storage, this paper formalizes the DPDP system model and security model. At the same time, we propose the first DPDP protocol which is provably secure under the assumption that the CDH problem is hard. Besides of the elimination of certificate management, our DPDP protocol has also flexibility and high efficiency. At the same time, the proposed DPDP protocol can realize private verification, delegated verification and public verification based on the client's authorization

More performance metric such as latency etc. can be considered. These performance metrics can be used to improve the performance of applications running in the cloud. These performance metric tests can be run on large EC2 instances. More performance metric such as latency etc. can be considered. During uploading and download user has to answer the security question and security question and answer are provided by user during the registration phase. So uploading/downloading operation if user is normal then he can answer that security question if he/she cannot answer that question thus using this we can provide more security. We can provide the security to upload data and the digest by using the encryption algorithm

REFERENCES

[1] H.Q. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, 2012. http://doi.ieeecomputersociety.org/10.1109/TSC.2012.35

[2] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, 5(2), pp. 220-232, 2012.

[3] Y. Zhu, G.J. Ahn, H. Hu, S.S. Yau, H.G. An, S. Chen, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Transactions on Services Computing, 2011. http://doi.ieeecomputersociety.org/10.1109/TSC.2011.51

[4] O. Goldreich, "Foundations of Cryptography: Basic Tools", Publishing House of Electronics Industry, Beijing, 2003, pp. 194-195.

[5] D. Boneh, M. Franklin, "Identity-based Encryption from the Weil Pairing", CRYPTO 2001, LNCS 2139, 2001, 213-229.

[6] S. Yu, K. Ren, W. Lou, "Attribute-based On-demand Multicast Group Setup with Membership Anonymity", Calculater Networks, 54(3), pp. 377-386, 2010.